

DMDC

DoD Enterprise Personnel Identity Protection



Prepared for:
PMR

March 2, 2004

Worldwide Leadership in Identity

Presented by:
Mary Dixon

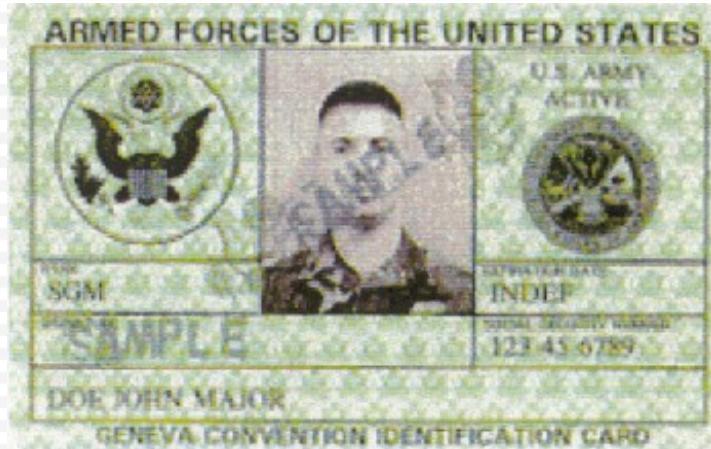
Purpose of the Brief

- **Define Personnel Identity Protection and why it's important to DoD**
- **Outline a series of IT systems and products that support Personnel Identity Protection, some of which you may not be familiar with**
- **Explain DoD's leadership position**
- **Overview of new DoD Directive for Personnel Identity Protection**

What is Personnel Identity Protection?

- **Establishment of identity is a basic business function - who are my employees, customers, suppliers**
- **In the past this was taken for granted - people were who they said they claimed to be**
- **Today assumptions about identity can create security issues**
- **Each business or government must take steps to provide assurance of identity - foundation of sound business practice**

Why Personnel Identity Protection is Important?



Military ID Card (\$75.00)

Counterfeits on the Internet

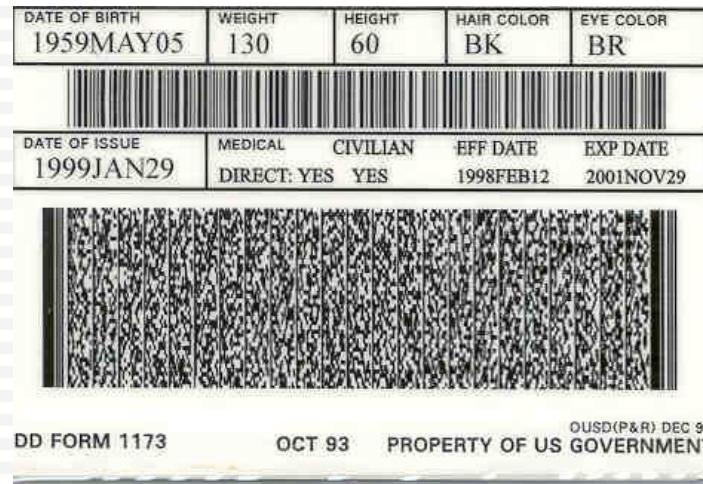


**Birth Certificates
(\$79.00)**



Social Security Cards (\$40.00)

Counterfeit Credentials are Common



- Fakes come as a package - with everything needed
- Overseas hundreds of fakes are detected

Courtesy USFK Provost Marshall

Personnel Identity Protection is a Process

- 1. Strong authentication of the individual**
 - A face to face interaction between the individual and a trusted agent
 - A business process that provides sufficient evidence of identity -- checks of public records, background investigations, examination of primary documents
- 2. Binding the identity to a management system**
 - A credential is the best linkage to the personnel identity protection system
- 3. Binding the credential to the individual**
 - Biometrics and PINs bind the credential to the person
 - Credential then becomes a proxy for digital/physical access given technology is used
- 4. Authentication of the credential at all access points**
 - Logical and Physical
- 5. Safeguarding identity information from unwarranted disclosure**

DoD is a World Leader in Personnel Identity Protection

We are good at this. Why? We follow the best

practices and have strong systems already in place.

Business Practice

System or Process

Proponent

Strong Authentication

RAPIDS/MEPCOM

P&R

Background vetting

ENTNAC/ADP

P&R/I

Identity Binding

RAPIDS

P&R

Digital Credential Issuance

RAPIDS/CA

P&R/NII

Identity Repository

DEERS

P&R

Biometric Capture &
Storage

DEERS/RAPIDS/DBID
S

P&R

Non-Digital Credentials

DEERS/RAPIDS/DBID
S

P&R

Also

We changed to higher Assurance Business Processes and continue to raise the bar...because we have to

- **Improved the vetting of recruits and employees**
- **Strengthened the procedures for issuing identification credentials**
- **Increased the use of technology on the CAC to enable more e-business processes**
- **Introduced wide-spread use of biometrics**
- **Facilitated multi-factor authentication for physical access**

Also
We developed a number of new systems and tools to support

Personnel Identity Protection in DoD

- **Common Access Card** - smart card with PKI Digital credentials
- **Defense Biometric Identification System (DBIDS)** - theater-wide physical access system
- **DoD National Visitors Center (DNVC)** - web based authentication for DoD ID credentials
- **Defense Cross-Credentialing Identification System (DCIS)** - authentication services across government agency and with private sector
- **Non-Combatant Evacuation Operations (NEO) Tracking System (NTS)** - tracks NEOs as they move through the evacuation process
- **Automated Repatriation Reporting System (ARRS)** - Tracks NEOs as they return to US

DoD Personnel Identity Protection Systems Common Access Card (CAC)

- **DoD Enterprise solution for digital credentials and e-Gov paperless transactions**
- **Fully integrated with RAPIDS and DEERS systems**
- **Mated with NII enterprise solution for PKI and directory services**
- **Full production - Infrastructure fully rolled out - 900 sites, 2000 workstations; Almost 4.0M cards issued**
- **Issuing cards with all functionality within target time parameters - 6-8 minutes (with 3 certs) - 12 minute total interaction time**
- **Finish initial issuance of 4.5M cards - target March 2004**

DoD Personnel Identity Protection Systems

Defense Biometric Identification System (DBIDS)

DBIDS is a personnel identity protection and force protection system that:

- **Uses existing DoD issued identification credentials**
- **Is scalable to cover a building, an installation, or an entire theater of operations**
- **Contains information on the individual, a digital photo, and a digital fingerprint**
- **Allows level of authentication to vary by threat level or at local commander's option**
- **Is rule driven - configurable by local authorities to meet their business rules for access**
- **Issues badges for individuals not authorized DoD credentials under DoD Instruction 1000.13**
- **Largest Physical Access System in DoD and largest use of biometrics for access in the Department**

DBIDS

Germany



Korea



- Korea - fully deployed 250K registrations
- Japan - planning on-going
- Europe - Registration over 175K+ - gates now operational
- Kuwait - system deployed -

Kuwait



DoD Personnel Identity Protection Systems

oD National Visitors Center (DNVC)

Authenticates

DoD ID Credential holders at DoD bases and facilities for physical access

DoD Cross-Credentialing Identification System

Authenticates

Federated Commercial and Government ID Credentials Holders within DoD and at each others' facilities

Features:

- Secure Web-based access within DoD and between Partners
- Signed delivery of authentication data including biometrics
- Trust server can be scaled to add federated

DoD National Visitors Center (DNVC)

Concept

- **Authentication of DoD Credentials increasing requirement**
- **Services need web based, enterprise-wide capability - anywhere, any credential requiring only a browser**
- **Use comprehensive DEERS/RAPIDS data store to provide information**
- **Incorporate biometrics - photo and fingerprint (fingerprint matching an option - requires reader and client software)**
- **Accommodates Members, retirees and families**
- **Links strong authentication to base access systems and local access policies**

DNVC Authentication Result - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Search Favorites Media

Address http://webdev.int.dmdc.osd.mil/appj/lymh/manual.do Go Links

DMDC Information and Technology for Better Decision Making

DNVC Authentication Result



Photo options: Print, Save, E-mail, Copy.

Name: Jane Elizabeth Johnson
Association: Navy Uniformed Service/Personnel
Photo: Photo Found
Fingerprint: Fingerprint Found

Compare Fingerprints...

[authenticate new visitor](#)

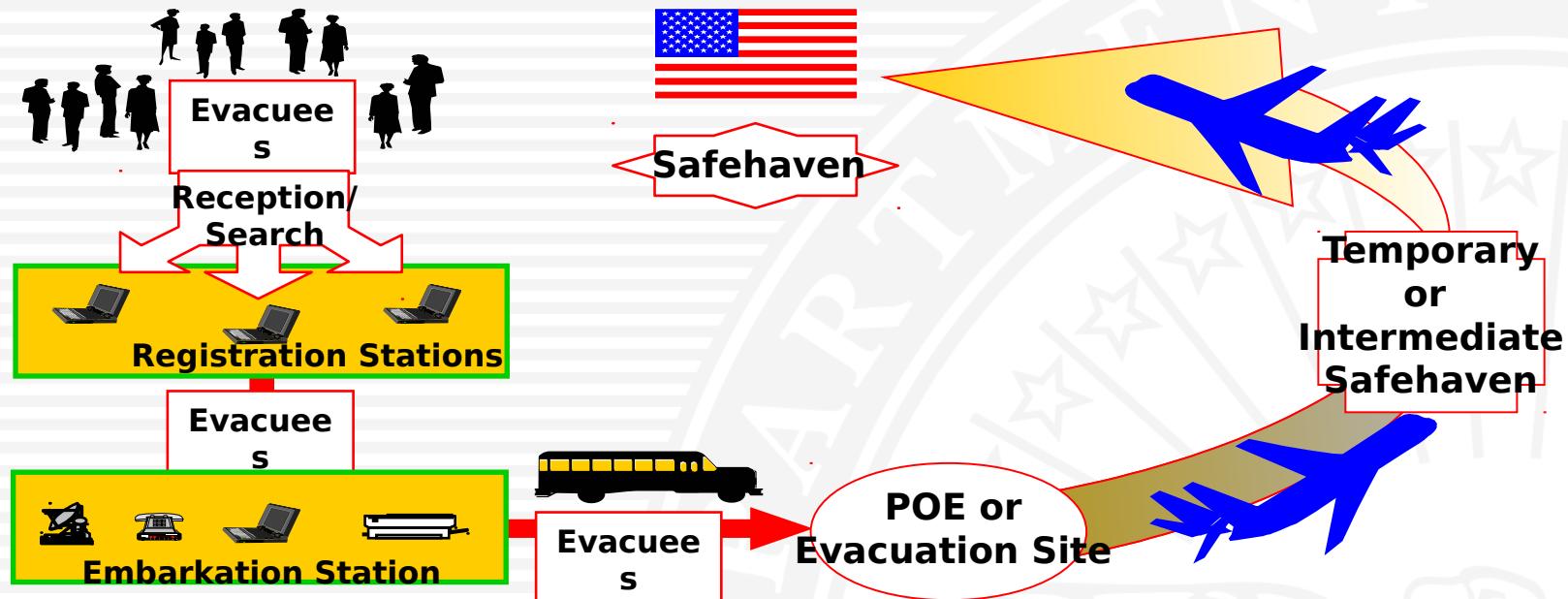
Done Internet

Defense Cross-Credentialing Identification System (DCIS)

Concept

- Extend DoD National Visitors Center capability to Defense Contractors and Other Federal Agencies
- Develop trust model to establish standards and practices for inclusion
- Develop capability so that Federated Partners retain control of employee/member data
- Develop data standards for participation
- Establish procedures for implementation and authentication options based on threat or local requirements

NEO Tracking System (NTS)



- Identifies and tracks noncombatant evacuees (NEOs) as they move through the evacuation pipeline
- Provides visibility of noncombatant personnel through up to date reports and queries
- Quickly and accurately collect and transmit information: bar code
• QR code ID

Automated Repatriation Reporting System (ARRS)

Evacuees from NEO Tracking System (NTS)



Repatriation Sites
13 Total



NTS Closure



Completed DD Form 2585



Repatriation Centers
6 Total



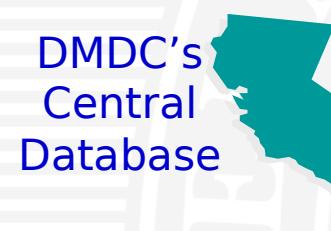
Updates & Queries



WEB Reports



DMDC's Central Database



- 1) DEERS Data
- 2) NEO Data (NTS)
- 3) DD Form 2585 (Repatriation Processing Sheet)

- Identify and track repatriates arriving in CONUS from overseas evacuation operations
- Mandatory scanning of the bar code NEO wristbands for returning evacuees to close out the NEO Tracking System (NTS) record
- Provide a nationwide repatriation database that can be used by key agencies to provide aid and support to repatriates
- Update the Repatriation Database from the DD Form 2585 (Repatriation Processing Sheet)

DOD Personnel Identity Protection - A structured approach to DoD ID Credentials

CAC



Base Cards



DoD ID Card

USAREUR/USAFFE Installation Pass	
Person Category	Expiration Date
Contractor	19 JUN 2006
Authorized Access To	Access Times
104th ASG Wide	0600-1800
Taylor Barracks	M-F
Sign-In Privileges	Access Authorized up to FP Condition
Not Authorized	BAVO
Name (Last,First,M.I.)	Rank/Grade/Title Personal ID No.
PARKER, Susan H.	MRS. 7008957632

**Logical &
Physical
Access &
Benefits**

**Civil Servants
Workers**

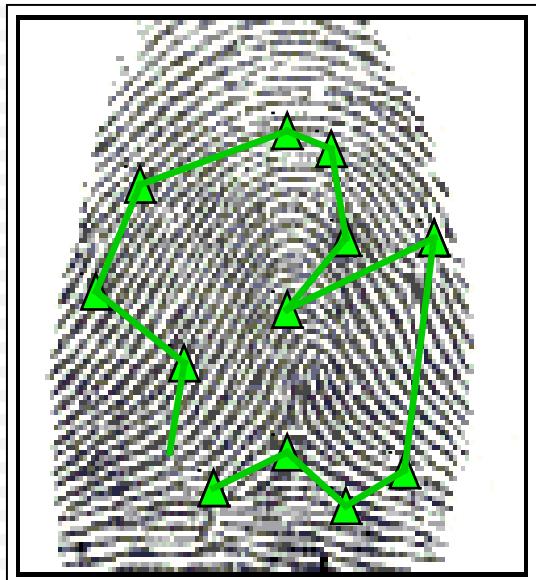
**Physical
Access
& Benefits**

Family Members

Physical Access Only

Base

Biometrics - Current Status



- **DEERS stores and uses over 5 million fingerprints for Active Duty, Reservists, Military retirees, DoD Civil Servants and Contractors**
- **MEPCOM collects about 200,000 ten prints sent to FBI each year**
- **DBIDS in Europe will enroll 400,000 currently at 175,000+**

Summary & Follow-on Actions to Strengthen Forward Progress

- Personnel Identity Protection is increasing in importance for provisioning benefits and for secure logical and physical access
- DoD has a strong program in place - world class
- Personnel Identity Protection supports President's Management Agenda and is Transformational Technology
- Consolidate policy, procedures, and responsibilities to secure strong personnel identity protection program
- Develop Directive per USD(P&R)

Overview of New Directive

- **Replaces 2 Directives and 1 Instruction**
- **Establishes Policy for PIP**
- **Assigns responsibilities for PIP**
 - USD P&R, USD I
 - NII/CIO/DISA
 - Services
- **Eliminates OIPT and JUSDAC, requires re-establishment of JUSPAC and JUSMAC via MOA, as necessary**
- **Establishes procedures for the protection of individual information credentialing of employees, members, and beneficiaries, use and content of credentials**
- **Designates DEERS as the definitive, authoritative data source for identity information for those individuals employed by or doing business with the DoD**
- **Designates RAPIDS as the Credentialing System**
- **Authorizes DBIDS, DCIS, DNVC and DNTS as PIP systems**
- **Incorporates IPMSCG and assigns dual oversight**

Questions?